

Claim Amendment Summary

Claims pending

- At time of the Action: Claims 1-49.
- After this Response: Claims 1-49.

Canceled or Withdrawn claims: none.

Amended claims: 14, 23, 42, and 43.

New claims: none.

Please amend claims 14, 23, 42, and 43 as follows:

1. (ORIGINAL) An authentication system comprising:

a host network configured to provide access to the Internet from a public location;

at least one authentication component communicatively linked with the host network and configured to enable authentication of individual users so that they can access the Internet through the host network, authentication being configured to take place in a manner that is independent of any user affiliation with any Internet Service Providers (ISPs);

at least one access module communicatively linked with the one authentication component and configured to enable a user to access the host network; and

an authentication database communicatively linked to the host network and containing user information that can be used to authenticate a user.

1 2. **(ORIGINAL)** The system of claim 1, wherein the
2 authentication database comprises a globally accessible authentication
3 database.

4
5 3. **(ORIGINAL)** The system of claim 2, wherein the user
6 authenticates directly with the authentication database.

7
8 4. **(ORIGINAL)** The system of claim 3, wherein the one
9 authentication component is configured to link a user directly to the
10 authentication database.

11
12 5. **(ORIGINAL)** The system of claim 3, wherein the one
13 authentication component is not privy to any authentication information
14 that passes between the user and the authentication database.

15
16 6. **(ORIGINAL)** The system of claim 3, wherein authentication
17 takes place between the user and the authentication database in a secure
18 manner.

19
20 7. **(ORIGINAL)** The system of claim 6, wherein the
21 authentication takes place using secure socket link (SSL) techniques.

22
23 8. **(ORIGINAL)** The system of claim 3, wherein the
24 authentication database is configured to notify the one authentication
25 component when a user has been properly authenticated.

1
2 **9. (ORIGINAL)** The system of claim 8, wherein the
3 authentication database is configured to provide user information to the one
4 authentication component after the user has been authenticated.
5

6 **10. (ORIGINAL)** The system of claim 9, wherein the user
7 information that is provided by the authentication database comprises
8 billing information.
9

10 **11. (ORIGINAL)** The system of claim 1, wherein the
11 authentication database comprises a locally accessible authentication
12 database.
13

14 **12. (ORIGINAL)** The system of claim 1, wherein the one
15 authentication component is configured to issue a unique token to each user
16 once the user is authenticated by the authentication database, the unique
17 token being provided for use with data packets that can be transmitted from
18 each user.
19

20 **13. (ORIGINAL)** The system of claim 1, wherein the one access
21 module is configured to enable the user to wirelessly access the host
22 network.
23
24
25

1 **14. (CURRENTLY AMENDED)** An authentication system for
2 providing authentication for users who desire to access the Internet, the
3 system comprising:

4 at least one host organization network configured to access the
5 Internet, the host organization network comprising one or more subnets
6 each of which comprising:

7 at least one server configured to receive data packets from
8 individual client computing devices and transmit the data packets to the
9 Internet; and

10 a plurality of public access points each of which configured to
11 receive wireless communication from a user that is using a client
12 computing device to wirelessly transmit data packets that are intended for
13 the Internet and provide the wirelessly transmitted data packets to the one
14 server before the data packets are transmitted to the Internet; and

15 at least one globally accessible authentication database that contains
16 information that can be used by the database to authenticate a user without
17 requiring the user to be affiliated with ~~a particular~~ at least one Internet
18 Service Provider (ISP).

19
20 **15. (ORIGINAL)** The system of claim 14, wherein the user
21 authenticates directly with the globally accessible authentication database.

22
23 **16. (ORIGINAL)** The system of claim 14, wherein the one
24 server is not privy to authentication information that is passed between the
25 client computing device and the globally accessible authentication database.

1
2 **17. (ORIGINAL)** The system of claim 14, wherein
3 authentication takes place between the client computing device and the
4 globally accessible database in an end-to-end secure manner.

5
6 **18. (ORIGINAL)** The system of claim 17, wherein the secure
7 manner comprises secure socket layer (SSL) techniques.

8
9 **19. (ORIGINAL)** The system of claim 14, wherein the globally
10 accessible authentication database is configured to notify the one server
11 when a user has been authenticated.

12
13 **20. (ORIGINAL)** The system of claim 19, wherein the globally
14 accessible authentication database is configured to provide user information
15 to the one server when the user has been authenticated.

16
17 **21. (ORIGINAL)** The system of claim 20, wherein the user
18 information that is provided to the one server by the globally accessible
19 authentication database comprises billing information.

20
21 **22. (ORIGINAL)** The system of claim 14, wherein the user is
22 unaffiliated with any Internet Service Providers (ISPs).

1 **23. (CURRENTLY AMENDED)** An authentication system for
2 providing authentication for users who desire to access the Internet, the
3 system comprising:

4 multiple wireless nodes through which the Internet can be accessed;

5 multiple access points with which the wireless nodes can
6 communicate;

7 a server configured to receive wireless communication from the
8 multiple access points, the server configured to enable authentication of
9 various users; and

10 at least one global authentication database that contains user
11 information that can be used to authenticate the users without requiring
12 the users to be affiliated with ~~a particular~~ at least one Internet Service
13 Provider (ISP).

14
15 **24. (ORIGINAL)** The system of claim 23, wherein the server is
16 configured to enable a user to log directly onto the one global
17 authentication database.

18
19 **25. (ORIGINAL)** The system of claim 24, wherein the server is
20 configured to present a web page having a link to the one global
21 authentication database.

22
23 **26. (ORIGINAL)** The system of claim 24, wherein the server is
24 not privy to any of the authentication information that gets passed between
25 the user and the one global authentication database.

1
2 **27. (ORIGINAL)** The system of claim 24, wherein the one
3 global authentication database is configured to notify the server after the
4 user has been authenticated.
5

6 **28. (ORIGINAL)** The system of claim 27, wherein the one
7 global authentication database is configured to provide user information to
8 the server after the user has been authenticated by the global authentication
9 database.
10

11 **29. (ORIGINAL)** The system of claim 23, wherein the server is
12 configured to issue a unique token to the user after the user is authenticated.
13

14 **30. (ORIGINAL)** The system of claim 29, wherein the server
15 encrypts the unique token before issuing it to the user.
16

17 **31. (ORIGINAL)** The system of claim 23, wherein the multiple
18 access points are arranged to define a wireless subnet.
19

20 **32. (ORIGINAL)** The system of claim 23, wherein the multiple
21 access points are deployed in a publicly accessible area.
22

23 **33. (ORIGINAL)** The system of claim 23, wherein the multiple
24 wireless nodes comprise mobile computing devices.
25

1 **34. (PREVIOUSLY PRESENTED)** A method of authenticating
2 a user for Internet access, the method comprising:
3 establishing a communication link between a mobile computing
4 device and a server that is configured to provide Internet access;
5 contacting a global authentication database that contains user
6 information that can be used to authenticate one or more users;
7 authenticating a user using the information that is contained in the
8 global authentication database, independent of any user affiliation with any
9 Internet Service Providers (ISPs);
10 notifying the server that the user has been authenticated; and
11 issuing a unique token to the user for use when sending data packets
12 to the server for transmission to the Internet.

13
14 **35. (ORIGINAL)** The method of claim 34, wherein the
15 communication link comprises at least one wireless link.

16
17 **36. (ORIGINAL)** The method of claim 34, wherein the
18 communication link comprises a wireless link that includes the mobile
19 computing device.

20
21 **37. (ORIGINAL)** The method of claim 34, wherein the
22 communication link comprises a wireless link that includes the server.

1 **38. (ORIGINAL)** The method of claim 34, wherein the
2 communication link comprises a wireless link that includes both the mobile
3 computing device and the server.

4
5 **39. (ORIGINAL)** The method of claim 34, wherein said
6 authenticating comprises authenticating the user using a secure protocol.

7
8 **40. (ORIGINAL)** The method of claim 39, wherein the server is
9 not privy to any authentication information that passes between the user
10 and the authentication database.

11
12 **41. (ORIGINAL)** The method of claim 34, wherein the server
13 comprises part of a publicly deployed and accessible host network.

14
15 **42. (CURRENTLY AMENDED)** One or more computer-
16 readable media having computer-readable instructions thereon which, when
17 executed by one or more computers, cause the computers to:

18 establish a wireless communication link between a mobile
19 computing device and a server that is configured to provide Internet access;

20 contact a global authentication database that contains user
21 information that can be used to authenticate one or more users;

22 authenticate a user using the information that is contained in the
23 global authentication database, independent of requiring the user to be
24 affiliated with a particular any Internet Service Provider (ISP);

25 notify the server that the user has been authenticated; and

1 issue a unique token to the user for use when sending data packets to
2 the server for transmission to the Internet.

3
4 **43. (CURRENTLY AMENDED)** A method of authenticating a
5 user for Internet access, the method comprising:

6 configuring multiple access points to receive wireless
7 communication from multiple wireless nodes through which the Internet
8 can be accessed, the multiple wireless nodes being capable of
9 communicating data packets that are intended for transmission to the
10 Internet;

11 configuring a server to wirelessly receive the data packets that are
12 communicated to the multiple access points; and

13 configuring a globally accessible database that includes information
14 that can be used to authenticate one or more users that desire to access the
15 Internet, authentication taking place in a manner that does not require the
16 one or more users to be affiliated with ~~a particular~~ at least one Internet
17 Service Provider (ISP).

18
19 **44. (ORIGINAL)** The method of claim 43 further comprising
20 using the globally accessible database to authenticate one or more users.

21
22 **45. (ORIGINAL)** The method of claim 44, wherein said using
23 comprises linking the user directly to the globally accessible database.
24
25

1 **46. (ORIGINAL)** The method of claim 44, wherein said using
2 comprises linking the user directly to the globally accessible database and
3 authenticating the user outside of the purview of the server.

4
5 **47. (ORIGINAL)** The method of claim 44, wherein said using
6 comprises linking the user directly to the globally accessible database and
7 notifying the server when the user has been authenticated.

8
9 **48. (ORIGINAL)** The method of claim 44 further comprising
10 issuing a user, once authenticated, a unique token that uniquely identifies
11 that user.

12
13 **49. (ORIGINAL)** The method of claim 43, wherein at least some
14 of the wireless nodes comprise mobile computing devices.
15
16
17
18
19
20
21
22
23
24
25